Jurnal Kejuruteraan 33(3) 2021: 733-739
https://doi.org/10.17576/jkukm-2021-33(3)-31

Complete Decompositions of Dihedral Groups and Group Based Key Exchange Protocol

Huey Voon Chen[a*] & Chang Seng Sin[a]

[a]Department of Mathematical and Actuarial Science,
Lee Kong Chian Faculty of Engineering & Science, Universiti Tunku Abdul Rahman, Malaysia

Corresponding author: chenhv@utar.edu.my

Received 29 January 2021, Received in revised form 09 March 2021
Accepted 09 April 2021, Available online 30 August 2021

ABSTRACT

This research is about the group coverings of subsets of finite non-abelian groups and its application in the field of cryptography. Group coverings of finite abelian groups has been researched over the years and it has many applications in various fields. The popularity of internet has increased rapidly and the application of cryptography become more important as it ensures the privacy and security of the users in the network. A cryptosystem is a structure consisting of several cryptographic primitives. Key exchange protocol is one of the cryptographic primitives that parties used to exchange a shared key. The group covering that we investigate in this paper is the complete decompositions of order t in dihedral group. Let D_{2n} be dihedral group of order 2 for positive integer n≥3. We show some constructions of complete decompositions of D_{2n} of order t for t∈{2,3,...,n}. Since D_{2n} is a non-abelian group, the hardness of the mathematical problems will be increased in designing a secure cryptosystem. By using the computational complete decomposition of dihedral group of order t search problem, two parties key exchange protocol is proposed without sharing any keys directly. Finally, we show that the proposed scheme is a secure communication between the authorized parties and protect the data from being disclosed to the third parties or hackers.

Keywords: Non-abelian group; Complete decompositions; Dihedral group; Key exchange protocol

INTRODUCTION

Group factorization is a popular research topic and it has attracted the attention of researchers over the years. They studied the factorization of a group into subsets with certain properties as they found some applications related to factoring group into subsets (Szabo and Sands, 2009). Zhou (2017) studied the multiple factorizations of cyclic groups. Some researchers looked into the exhaustion numbers of subsets of finite groups. Chen and Chin (2017) investigated some properties of exhaustive and non-exhaustive subsets of finite groups. Wong et al. (2018) studied the exhaustion 2-subsets in dihedral groups of order 2p. The existence of complete decompositions of cyclic group $\mathbb{Z}_n$, which can be used to construct codes in cyclic groups over a binary alphabet was shown in Chin and Chen (2018).

There are several applications of group factorization found in different fields such as cryptography. For instance, in Magliveras et al. (2002) and Magliveras (2002) proposed some public key cryptosystems by using group factorization as a trapdoor. Baba et al. (2011) constructed a cryptosystem defined over non-abelian groups based on the factorization problem. Lee (2005) showed that some of the cryptographic tools that developed based on finite groups still useful in infinite groups by providing some constructions. Cong et al. (2019) proposed a new simplified secure encryption schemes based on group factorization problem with higher efficiency.

The internet is one of the main medium to reach everyone on the globe nowadays. The application of cryptography become more important as it ensures the privacy and security of the users in the network. A cryptosystem is a structure consisting of several cryptographic primitives. Cryptographic primitives are used in insecure communication channels such as virtual private network, encrypted web traffic to exchange secret information. Key exchange protocol is one of the cryptographic primitives that parties used to exchange a shared key. Boyd and Anish (2003) discussed the protocols for authentication and key establishment and highlighted that are the foundation for security of communications. Diffie and Hellman (1976) developed the idea of asymmetric key exchange protocol. They proposed Diffie-Hellman key exchange protocol using the hardness of solving discrete logarithm problem. Rivest et al. (1978) constructed the RSA encryption scheme, where the security is based on integer factorization problem. ElGamal (1984) modified the Diffie-Hellman key exchange protocol to ElGamal key exchange protocol. In addition, he constructed a new digital signature scheme based on the difficulty of solving discrete logarithm problem over finite fields. Generally, a hard problem is defined as a particular problem that cannot be solved in polynomial time. Shor (1997) proposed an algorithm that can feasibly solved many conventional number theories based hard problems such as integer factorization problem and discrete logarithm problem. Therefore, the security of the schemes that constructed based on these problems become questionable (Zhang et al., 2004) and the era of postquantum cryptography emerged. Over the last decade, researchers started to construct some cryptographic primitives in lattice-based, code-based, hash-based and etc. Rawat and Deshmukh (2019) proposed key exchange approach based on modular arithmetic equations. Peng et al. (2020) proposed a new lightweight key exchange protocol based on T-tensor product, which required lower power consumption with higher speed. The self-certified public keys based group key agreement protocol proposed by Gupta el at. (2018) has capability to overcome the certificate management problem. Gu and Zheng (2014) proposed some hard problems which are related to the factorization problem. They showed that these hard problems are useful by providing some constructions of cryptographic primitives. This motivated us to search for new hard problem that might remain secure under attacks using non-abelian groups.

This paper aims to investigate the complete decompositions of dihedral groups D_{2n} and its application. We first show some constructions of complete decompositions of D_{2n} of order t for $t \in \{3,4,\ldots,n\}$. Next, we propose a key exchange protocol based on the complete decompositions of dihedral groups of order t and show that the proposed scheme is secure. Let us recall the definition of complete decompositions of G of order t. Let G be a finite non-abelian group. Let $B_1, \ldots, B_t$ be nonempty subsets of G which are pairwise disjoint for integer $t \geq 2$. $(B_1, \ldots, B_t)$ is a complete decomposition of G of order t if the subsets product $B_{i1} \ldots B_{it} = \{b_{i1} \ldots b_{it} \mid b_{ij} \in B_{ij}, \text{j} = 1, 2, \ldots, t\}$ coincides with G, where $\{B_{i1}, \ldots, B_{it}\} = \{B_1, \ldots, B_t\}$ and the B_{ij} are all distinct. Throughout this paper, we let G be dihedral groups, D_{2n}, for $n \geq 3$. It is clear that $D_{2n} = \langle r,s \mid r^n = s^2 = 1, sr = r^{-1} s\rangle = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1} s\}$ is a non-abelian group of order 2_n, where $\langle r\rangle = \{1, r, \ldots, r^{n-1}\}$ is a cyclic subgroup of D_{2n} of order n.

METHODOLOGY

Some Constructions on Complete Decompositions of Dihedral Groups

Let $A, B \subseteq D_{2n}$. If $A \cap B = \emptyset$ and either $|A| = 1$ or $|B| = 1$, then $|AB| < 2n$ and hence (A, B) is not a complete decomposition of D_{2n} of order 2. Let us consider the subsets A and B such that $|A|, |B| \in \{2,3, \ldots, 2n-2\}$. In this section, we will show some constructions of complete decompositions of D_{2n} of order t for $t \in \{2,3, \ldots, n\}$.

Proposition 1. Let $A = \{1, r^{v+1}, r^{v+2}, \ldots, r^{n-1}, r^v s, r^{v+1} s, \ldots, r^{n-1} s\}$ and $B = \{r, r^2, \ldots, r^v, s, rs, \ldots, r^{v-1} s\}$ be the subsets of D_{2n}, where $v \in \{1,2, \ldots, n-2\}$, $|A| = 2n - 2v$ and $|B| = 2v$. Then (A, B) is a complete decomposition of D_{2n} of order 2 for $n \geq 3$.

Proof.
Let $L_1 = \{r^{v+1}, r^{v+2}, \ldots, r^{n-1}\} \subseteq A$ and $L_2 = \{r, r^2, \ldots, r^v\} \subseteq B$. We have $L_1 L_2 = \{r^{v+1}, r^{v+2}, \ldots, r^{n-1}\}\{r, r^2, \ldots, r^v\} = \{r^{v+2}, r^{v+3}, \ldots, r^{n-1}\} \cup \{1, r, \ldots, r^{v-1}\}$.

Note that $1 \in A$, therefore $\{r, r^2, \ldots, r^v\} \subseteq AB$. It is clear that $\langle r\rangle \setminus (L_1 L_2 \cup \{r^v\}) = \{r^{v+1}\}$. Observe that $r^{v+1} s \in A$ and $s \in B$. Thus, we have $(r^{v+1} s)(s) = r^{v+1} \in AB$. Therefore, $\{r^v, r^{v+1}, \ldots, r^{v+n-1}\} = \langle r\rangle \subseteq AB$. It remains to show that $\langle r\rangle s \subseteq AB$. Let $L_3 = \{s, rs, \ldots, r^{v-1} s\} \subseteq B$. We see that $L_1 L_3 = \{r^{v+1}, r^{v+2}, \ldots, r^{n-1}\}\{s, rs, \ldots, r^{v-1} s\}$
$= \{r^{v+1} s, r^{v+2} s, \ldots, r^{n-1} s\} \cup \{s, rs, \ldots, r^{v-2} s\}$.
Clearly $\langle r\rangle s \setminus L_1 L_3 = \{r^v s, r^{v+n-1} s\}$. Observe that $\{r^v s, r^{v+1} s\} \subseteq A$ and $r \in B$. Therefore, we have $\{r^v s, r^{v+1} s\} r = \{r^{v+n-1} s, r^{v+n} s\} = \{r^v s, r^{v-1} s\} \subseteq AB$. Thus, $\{r^{v-1} s, r^v s, \ldots, r^{v+n-2} s\} = \langle r\rangle s \subseteq AB$. Hence, we conclude that (A, B) is a complete decomposition of D_{2n} of order 2.

Note that the elements are non-commutative in dihedral group. We remark that if $(B_1, B_2, \dots, B_t)$ is a complete decomposition of D_{2n} of order t, it does not imply that $(B_{j_1}, B_{j_2}, \dots, B_{j_t})$ is a complete decomposition of D_{2n} of order t, where $\{B_{j_1}, B_{j_2}, \dots, B_{jt}\} = \{B_1, B_2, \dots, B_t\}$.

Proposition 2. Let $n \geq 3$ and $A_1, A_2, A_3 \subseteq D_{2n}$, where $A_1 = \{1, r\}, A_2 = \{s, rs\}$ and $A_3 = \{r^2, r^3, \dots, r^{n-1}, r^2 s, r^3 s, \dots, r^{n-1} s\}$. Then (A_1, A_2, A_3) is a complete decomposition of D_{2n} of order 3.

Proof.
We first compute $A_1 A_2$ as follows:

$$A_1 A_2 = \{1, r\}\{s, rs\}$$

and followed by

$$\begin{aligned} &A_1 A_2 A_3 \\ &= \{s, rs, r^2 s\}\{r^2, r^3, \dots, r^{n-1}, r^2 s, r^3 s, \dots, r^{n-1} s\} \\ &= \{r^{n-2} s, r^{n-3} s, \dots, rs, r^{n-2}, r^{n-3}, \dots, r, \\ &\qquad r^{n-1} s, r^{n-2} s, \dots, r^2 s, r^{n-1}, r^{n-2}, \dots, r^2, \\ &\qquad r^n s, r^{n-1} s, \dots, r^3 s, r^n, r^{n-1}, \dots, r^3\} \\ &= \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1} s\} = D_{2n}. \end{aligned}$$

Hence, (A_1, A_2, A_3) is a complete decomposition of D_{2n} of order 3.

In the following, we show the constructions of complete decomposition of D_{2n} of order $k \in \{4, 5, \dots, n\}$ using the subsets

$$\begin{aligned} A_1 &= \{1, r\}; \\ A_2 &= \{s, rs\}; \\ A_i &= \{r^{i-1}, r^{i-1} s\} \text{ for } i \in \{3, 4, \dots, k-1\}; \\ A_k &= \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1} s, r^k s, \dots, r^{n-1} s\}. \end{aligned}$$

Proposition 3. Let $n \geq 7$. There exists a complete decomposition of D_{2n} of order k for $k \in \{4, 5, 6, 7\}$.

Proof.
Let

$$\begin{aligned} A_1 &= \{1, r\}; \qquad A_2 = \{s, rs\}; \\ A_i &= \{r^{i-1}, r^{i-1} s\}, \qquad \text{for } i \in \{3, 4, \dots, k-1\}; \\ A_k &= \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1} s, r^k s, \dots, r^{n-1} s\} \end{aligned}$$

where $A_1, A_2, \dots, A_k \subseteq D_{2n}$. Note that $A_1 A_2 = \{1, r\}\{s, rs\} = \{s, rs, r^2 s\}$. We compute $A_1 A_2 A_3$ as follows:

$A_1 A_2 A_3 = \{s, rs, r^2 s\}\{r^2, r^2 s\} = \{1, r^{n-2}, r^{n-1}, s, r^{n-2} s, r^{n-1} s\}$.

When $k = 4$, we have $A_4 = \{r^3, r^4, \dots, r^{n-1}, r^3 s, r^4 s, \dots, r^{n-1} s\}$. We compute $A_1 A_2 A_3 A_4$ as follows:

$$\begin{aligned} A_1 A_2 A_3 A_4 &= \{1, r^{n-2}, r^{n-1}, s, r^{n-2} s, r^{n-1} s\} \\ &\qquad \{r^3, r^4, \dots, r^{n-1}, r^3 s, r^4 s, \dots, r^{n-1} s\} \\ &= \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1} s\} = D_{2n}. \end{aligned}$$

Hence, (A_1, A_2, A_3, A_4) is a complete decomposition of D_{2n} of order 4. By using the similar way, it can be shown that the results hold for the cases $k = 5, 6, 7$.

Lemma 4. Let $n \geq 8,\ k \in \{8, 9, \dots, n\}$ and $A_i = \{r^{i-1}, r^{i-1} s\} \subseteq D_{2n}$ for $i \in \{3, 4, \dots, k-1\}$. Then $A_3 A_4 \dots A_{k-1} =$
$\{r^{-c+5}, r^{-c+11}, r^{-c+13}, \dots, r^{c-9}, r^{c-7}, \dots, r^{c-1}\} \cup$
$\{r^{-c+5} s,\ r^{-c+11} s,\ r^{-c+13} s,$
$\dots, r^{c-9} s, r^{c-7} s, r^{c-1} s\}$, where $c = \frac{(k-2)(k-1)}{2}$.

Proof.
Let us start by showing the base case $k = 8$ is true. We compute $A_3 A_4 A_5 A_6 A_7$ as follows:

$$\begin{aligned} &A_3 A_4 = \{r^2, r^2 s\}\{r^3, r^3 s\} = \{r^{-1}, r^5, r^{-1} s, r^5 s\}; \\ &A_3 A_4 A_5 = \{r^{-1}, r^5, r^{-1} s, r^5 s\}\{r^4, r^4 s\} \\ &= \{r^{-5}, r, r^3, r^9, r^{-5} s, rs, r^3 s, r^9 s\}; \\ &A_3 A_4 A_5 A_6 \\ &= \{r^{-5}, r, r^3, r^9, r^{-5} s, rs, r^3 s, r^9 s\}\{r^5, r^5 s\} \\ &= \{r^{-10}, r^{-4}, r^{-2}, 1, r^4, r^6, r^8, r^{14}, \\ &\qquad r^{-10} s, r^{-4} s, r^{-2} s, s, r^4 s, r^6 s, r^8 s, r^{14} s\}; \end{aligned}$$

$$\begin{aligned} &A_3 A_4 A_5 A_6 A_7 \\ &\quad = \{r^{-10}, r^{-4}, r^{-2}, 1, r^4, r^6, r^8, r^{14}, r^{-10} s, r^{-4} s, \\ &\qquad r^{-2} s, s, r^4 s, r^6 s, r^8 s, r^{14} s\}\{r^6, r^6 s\} \\ &\quad = \{r^{-16}, r^{-10}, r^{-8}, r^{-6}, r^{-4}, r^{-2}, 1, r^2, r^4, r^6, r^8, \\ &\qquad r^{10}, r^{12}, r^{14}, r^{20}\} \cup \\ &\qquad \left\{\begin{matrix} r^{-16} s, r^{-10} s, r^{-8} s, r^{-6} s, r^{-4} s, r^{-2} s, s, r^2 s, \\ r^4 s, r^6 s, r^8 s, r^{10} s, r^{12} s, r^{14} s, r^{20} s \end{matrix}\right\}. \end{aligned}$$

When $k = 8$, we see that statement is true and the base case holds. Suppose that the statement holds for the case $k = m$. By assumption, we see that

$$\begin{aligned} &A_3 A_4 \dots A_{m-1} \\ &= \{r^{-\frac{(m-2)(m-1)}{2}+5}, r^{-\frac{(m-2)(m-1)}{2}+11}, \\ &\quad r^{-\frac{(m-2)(m-1)}{2}+13}, \dots, r^{\frac{(m-2)(m-1)}{2}-9}, \\ &\quad r^{\frac{(m-2)(m-1)}{2}-7}, r^{\frac{(m-2)(m-1)}{2}-1}\} \cup \\ &\quad \{r^{-\frac{(m-2)(m-1)}{2}+5} s, r^{-\frac{(m-2)(m-1)}{2}+11} s, \\ &\quad r^{-\frac{(m-2)(m-1)}{2}+13} s, \dots, \\ &\quad r^{\frac{(m-2)(m-1)}{2}-9} s, r^{\frac{(m-2)(m-1)}{2}-7} s, r^{\frac{(m-2)(m-1)}{2}-1} s\} \\ &= B_1 \cup B_1 s, \end{aligned}$$

where

$$\begin{aligned} B_1 = \{&r^{-\frac{(m-2)(m-1)}{2}+5}, r^{-\frac{(m-2)(m-1)}{2}+11}, \\ &r^{-\frac{(m-2)(m-1)}{2}+13}, \dots, \\ &r^{\frac{(m-2)(m-1)}{2}-9}, r^{\frac{(m-2)(m-1)}{2}-7}, r^{\frac{(m-2)(m-1)}{2}-1}\}. \end{aligned}$$

Next, we show that the statement is also true for $k = m + 1$. Note that $A_m = \{r^{m-1}, r^{m-1} s\}$ and $A_3 A_4 \dots A_m = B_1 A_m \cup B_1 s A_m$. We compute $B_1 A_m$ and $B_1 s A_m$ as follows:

$$\begin{aligned} &B_1 A_m \\ &= \{r^{-\frac{(m-2)(m-1)}{2}+5+(m-1)}, r^{-\frac{(m-2)(m-1)}{2}+11+(m-1)}, \\ &\quad r^{-\frac{(m-2)(m-1)}{2}+13+(m-1)}, \dots, \\ &\quad r^{\frac{(m-2)(m-1)}{2}-9+(m-1)}, r^{\frac{(m-2)(m-1)}{2}-7+(m-1)}, \\ &\quad r^{\frac{(m-2)(m-1)}{2}-1+(m-1)}\}\{1, s\} \\ &= C_1 \cup C_1 s \end{aligned}$$

$$
\begin{aligned}
&B_1sA_m\\
&= \{r^{-\frac{(m-2)(m-1)}{2}+5}s, r^{-\frac{(m-2)(m-1)}{2}+11}s,\\
&\quad r^{-\frac{(m-2)(m-1)}{2}+13}s, \dots, r^{\frac{(m-2)(m-1)}{2}-9}s,\\
&\quad r^{\frac{(m-2)(m-1)}{2}-7}s, r^{\frac{(m-2)(m-1)}{2}-1}s\}\\
&\quad \{r^{m-1}, r^{m-1}s\}\\
&= \{r^{-\frac{(m-2)(m-1)}{2}+5-(m-1)}, r^{-\frac{(m-2)(m-1)}{2}+11-(m-1)},\\
&\quad r^{-\frac{(m-2)(m-1)}{2}+13-(m-1)}, \dots,\\
&\quad r^{\frac{(m-2)(m-1)}{2}-9-(m-1)}, r^{\frac{(m-2)(m-1)}{2}-7-(m-1)},\\
&r^{\frac{(m-2)(m-1)}{2}-1-(m-1)}\}\{1, s\}\\
&= D_1 \cup D_1s,
\end{aligned}
$$

where

$$
\begin{aligned}
C_1 = \{&r^{-\frac{m(m-1)}{2}+2m+3},\\
&r^{-\frac{m(m-1)}{2}+2m+9}, \dots, r^{-\frac{m(m-1)}{2}+2m+11},\\
&\dots, r^{\frac{m(m-1)}{2}-9}, r^{\frac{m(m-1)}{2}-7}, \dots, r^{\frac{m(m-1)}{2}-1}\},
\end{aligned}
$$

$$
\begin{aligned}
&D_1\\
&= \{r^{-\frac{m(m-1)}{2}+5}, r^{-\frac{m(m-1)}{2}+11}, r^{-\frac{m(m-1)}{2}+13}, \dots,\\
&\quad r^{\frac{m(m-1)}{2}-9}, r^{\frac{m(m-1)}{2}-7}, r^{\frac{m(m-1)}{2}-1}\}.
\end{aligned}
$$

Thus, we have

$$
\begin{aligned}
&C_1 \cup D_1\\
&= \{r^{-\frac{m(m-1)}{2}+5}, r^{-\frac{m(m-1)}{2}+11}, r^{-\frac{m(m-1)}{2}+13}, \dots,\\
&r^{\frac{m(m-1)}{2}-9}, r^{\frac{m(m-1)}{2}-7}, r^{\frac{m(m-1)}{2}-1}\},\\
&C_1s \cup D_1s\\
&= \{r^{-\frac{m(m-1)}{2}+5}s, r^{-\frac{m(m-1)}{2}+11}s, r^{-\frac{m(m-1)}{2}+13}s,\\
&\quad \dots, r^{\frac{m(m-1)}{2}-9}s, r^{\frac{m(m-1)}{2}-7}s, r^{\frac{m(m-1)}{2}-1}s\}.
\end{aligned}
$$

Note that $A_3A_4 \dots A_m = C_1 \cup D_1 \cup C_1s \cup D_1s$. Thus, the statement holds for $k = m + 1$. By mathematical induction, we conclude that the statement holds for $k \in \{8, 9, \dots, n\}$.

Theorem 5. Let $n \geq 8$. There exists a complete decomposition of D_{2n} of order k for $k \in \{8, 9, \dots, n\}$.

Proof.

Let $A_1 = \{1, r\}$, $A_2 = \{s, rs\}$, $A_i = \{r^{i-1}, r^{i-1}s\}$ for $i \in \{3,4, \dots, k-1\}$ and $A_k = \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^ks, \dots, r^{n-1}s\}$ be the subsets of D_{2n}. We first compute

$$A_1A_2 = \{1, r\}\{s, rs\} = \{s, rs, r^2s\}.$$

Let $c = \frac{(k-2)(k-1)}{2}$. By Lemma 4, we see that

$$
\begin{aligned}
&A_3A_4 \dots A_{k-1}\\
&= \{r^{-c+5}, r^{-c+11}, r^{-c+13}, \dots, r^{c-9}, r^{c-7}, r^{c-1}\} \cup\\
&\{r^{-c+5}s, r^{-c+11}s, r^{-c+13}s, \dots, r^{c-9}s, r^{c-7}s, r^{c-1}s\}\\
&= L_1 \cup L_2,
\end{aligned}
$$

where

$$L_1 = \{r^{-c+5}, r^{-c+11}, r^{-c+13}, \dots, r^{c-9}, r^{c-7}, r^{c-1}\}$$

and

$$
\begin{aligned}
&L_2\\
&= \{r^{-c+5}s, r^{-c+11}s, r^{-c+13}s, \dots, r^{c-9}s, r^{c-7}s, r^{c-1}s\}.
\end{aligned}
$$

Now, we compute $A_1A_2L_1 \subseteq A_1A_2 \dots A_{k-1}$ and $A_1A_2L_2 \subseteq A_1A_2 \dots A_{k-1}$ as follows:

$$
\begin{aligned}
&A_1A_2L_1\\
&= \{s, rs, r^2s\}\{r^{-c+5}, r^{-c+11}, r^{-c+13}, \dots, r^{c-9}, r^{c-7}, r^{c-1}\}\\
&= \{r^{n-c+1}s, r^{n-c+2}s, r^{n-c+3}s\}\\
&\cup \{r^{n-c+7}s, r^{n-c+8}s, \dots, r^{n+c-9}s\} \cup\\
&\qquad \{r^{n+c-5}s, r^{n+c-4}s, r^{n+c-3}s\}\\
&= P_1 \cup P_2 \cup P_3;\\
&A_1A_2L_2 = \{s, rs, r^2s\}\{r^{-c+5}s, r^{-c+11}s, r^{-c+13}s,\\
&\qquad \dots, r^{c-9}s, r^{c-7}s, r^{c-1}s\}\\
&= \{r^{n-c+1}, r^{n-c+2}, r^{n-c+3}\}\\
&\qquad\qquad \cup \{r^{n-c+7}, r^{n-c+8}, \dots, r^{n+c-9}\} \cup\\
&\qquad \{r^{n+c-5}, r^{n+c-4}, r^{n+c-3}\}\\
&= M_1 \cup M_2 \cup M_3,
\end{aligned}
$$

where

$$
\begin{aligned}
P_1 &= \{r^{n-c+1}s, r^{n-c+2}s, r^{n-c+3}s\},\\
P_2 &= \{r^{n-c+7}s, r^{n-c+8}s, \dots, r^{n+c-9}s\},\\
P_3 &= \{r^{n+c-5}s, r^{n+c-4}s, r^{n+c-3}s\},\\
M_1 &= \{r^{n-c+1}, r^{n-c+2}, r^{n-c+3}\},\\
M_2 &= \{r^{n-c+7}, r^{n-c+8}, \dots, r^{n+c-9}\},
\end{aligned}
$$

$$M_3 = \{r^{n+c-5}, r^{n+c-4}, r^{n+c-3}\}.$$

Now, we compute $P_1A_k, P_2A_k, \dots, P_6A_k \subseteq A_1A_2 \dots A_k$ as follows:

$$
\begin{aligned}
&P_1A_k\\
&= \{r^{n-c+1}s, r^{n-c+2}s, r^{n-c+3}s\}\\
&\quad \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^ks, \dots, r^{n-1}s\}\\
&= \{r^{n-c+2}, r^{n-c+3}, \dots, r^{2n-c-k+4}\}\\
&\cup \{r^{n-c+2}s, r^{n-c+3}s, \dots, r^{2n-c-k+4}s\}\\
&= R_1;
\end{aligned}
$$

$$
\begin{aligned}
&P_2A_k\\
&= \{r^{n-c+7}s, r^{n-c+8}s, r^{n+c+9}s\}\\
&\quad \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^ks, \dots, r^{n-1}s\}\\
&= \{r^{n-c+8}, r^{n-c+9}, \dots, r^{2n+c-k-8}\}\\
&\cup \{r^{n-c+8}s, r^{n-c+9}s, \dots, r^{2n+c-k-8}s\}\\
&= R_2;
\end{aligned}
$$

$$
\begin{aligned}
&P_3A_k\\
&= \{r^{n+c-5}s, r^{n+c-4}s, r^{n+c-3}s\}\\
&\quad \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^ks, \dots, r^{n-1}s\}\\
&= \{r^{n+c-4}, r^{n+c-3}, \dots, r^{2n+c-k-2}\}\\
&\cup \{r^{n+c-4}s, r^{n+c-3}s, \dots, r^{2n+c-k-2}s\}\\
&= R_3;
\end{aligned}
$$

$$
\begin{aligned}
&M_1A_k\\
&= \{r^{n-c+1}, r^{n-c+2}, r^{n-c+3}\}\\
&\quad \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^ks, \dots, r^{n-1}s\}\\
&= \{r^{n-c+k}, r^{n-c+k+1}, \dots, r^{2n-c+2}\}\\
&\cup \{r^{n-c+k}s, r^{n-c+k+1}s, \dots, r^{2n-c+2}s\}\\
&= R_4;
\end{aligned}
$$

$$\begin{aligned} &M_2A_k \\ &= \{r^{n-c+7}, r^{n-c+8}, \dots, r^{n+c-9}\} \\ &\quad \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^k s, \dots, r^{n-1}s\} \\ &= \{r^{n-c+k+6}, r^{n-c+k+7}, \dots, r^{2n+c-10} \\ &\cup \{r^{n-c+k+6}s, r^{n-c+k+7}s, \dots, r^{2n+c-10}s\} \\ &= R_5; \end{aligned}$$

$$\begin{aligned} &M_3A_k \\ &= \{r^{n+c-5}, r^{n+c-4}, r^{n+c-3}\} \\ &\quad \{r^{k-1}, r^k, \dots, r^{n-1}, r^{k-1}s, r^k s, \dots, r^{n-1}s\} \\ &= \{r^{n+c-k-6}, r^{n+c-k-5}, \dots, r^{2n+c-4}\} \\ &\cup \{r^{n+c-k-6}s, r^{n+c-k-5}s, \dots, r^{2n+c-4}s\} \\ &= R_6. \end{aligned}$$

Note that $A_1A_2 \dots A_k = R_1 \cup R_2 \cup R_3 \cup R_4 \cup R_5 \cup R_6$. Observe that

$$\begin{aligned} &R_2 \\ &= \{r^{n-c+8}, r^{n-c+9}, \dots, r^{2n+c-k-8}\} \\ &\cup \{r^{n-c+8}s, r^{n-c+9}s, \dots, r^{2n+c-k-8}s\}, \end{aligned}$$

where $|\{r^{n-c+8}, r^{n-c+9}, \dots, r^{2n+c-k-8}\}| = |\{r^{n-c+8}s, r^{n-c+9}s, \dots, r^{2n+c-k-8}s\}| = n + 2c - k - 15 = n + k^2 - 2k - 15 \geq n$ for $k \in \{8, 9, \dots, n\}$. This shows that there exists a complete decomposition of D_{2n} of order k for $k \in \{8, 9, \dots, n\}$.

APPLICATION IN CRYPTOGRAPHY

Data communication security is essential since everyone has access to all valuable data using internet. We need to ensure the data being communicated between the authorized parties and protect the data from being disclosed to the third parties or hackers. If two parties wish to exchange encrypted data, each must be equipped to encrypt messages to be sent and decrypt messages received.

From the previous section, it is clear that there exists a complete decomposition of D_{2n} of order t for $t \in \{2,3,\dots,n\}$. Thus, $B_1 \dots B_t = D_{2n}$ for $t \in \{2,3,\dots,n\}$. By using Matlab, we generated all the possible 368 complete decompositions of D_8 of order 3. Since dihedral group is a non-abelian group, the subsets product are not commutative. Hence, we checked the subsets product of $B_1 B_2 B_3$ and $B_2 B_1 B_3$ and found that there are 17 out of 368 constructions indicated that $B_1 B_2 B_3 \neq B_2 B_1 B_3$. This showed that the order of the subsets is important and its noncommutative properties is useful to create key exchange protocol. In the following, a key exchange protocol based on the computational complete decomposition of non-abelian group of order t search problem between two parties is proposed.

Computational Complete Decomposition of Non-abelian Group of Order t Search Problem: Let G be a finite non-abelian group. Given B_1, ..., B_{t-1} and G where the subsets

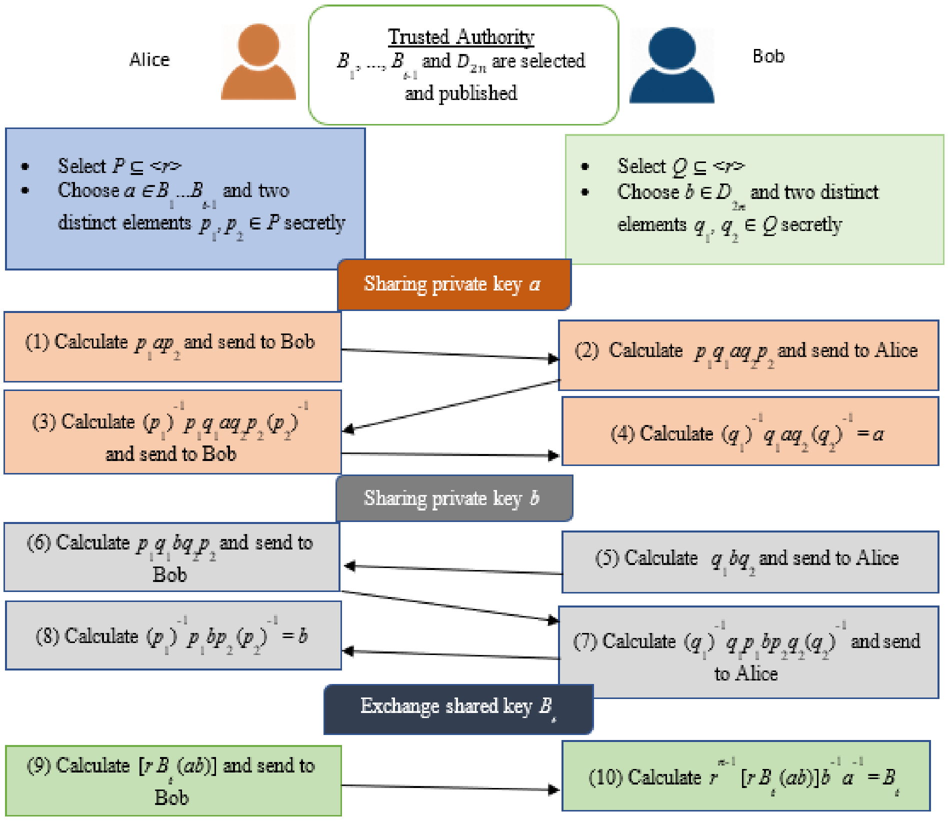
Alice
Trusted Authority
$B_1, \dots, B_{t-1}$ and D_{2n} are selected and published
Bob
Select $P \subseteq \langle r \rangle$
Choose $a \in B_1 \dots B_{t-1}$ and two distinct elements $p_1, p_2 \in P$ secretly
Select $Q \subseteq \langle r \rangle$
Choose $b \in D_{2n}$ and two distinct elements $q_1, q_2 \in Q$ secretly
Sharing private key a
(1) Calculate $p_1 a p_2$ and send to Bob
(2) Calculate $p_1 q_1 a q_2 p_2$ and send to Alice
(3) Calculate $(p_1)^{-1} p_1 q_1 a q_2 p_2 (p_2)^{-1}$ and send to Bob
(4) Calculate $(q_1)^{-1} q_1 a q_2 (q_2)^{-1} = a$
Sharing private key b
(6) Calculate $p_1 q_1 b q_2 p_2$ and send to Bob
(5) Calculate $q_1 b q_2$ and send to Alice
(8) Calculate $(p_1)^{-1} p_1 b p_2 (p_2)^{-1} = b$
(7) Calculate $(q_1)^{-1} q_1 p_1 b p_2 q_2 (q_2)^{-1}$ and send to Alice
Exchange shared key B_t
(9) Calculate $[r B_t (ab)]$ and send to Bob
(10) Calculate $r^{n-1} [r B_t (ab)] b^{-1} a^{-1} = B_t$

FIGURE 1. Two parties key exchange protocol using the Computational Complete Decomposition of Dihedral Groups Order t Search Problem

product B_1 ... B_{t-1} is a proper subset of G. Find B_t such that the subsets product B_1 ... B_t = G, where B_1, ..., $B_t \subseteq G$ and all the subsets are pairwise disjoint.

The non-abelian group that we focused is dihedral group D_{2n}. The subsets B_1, ..., B_{t-1} and the dihedral groups D_{2n} are selected and published first to both Alice and Bob. Suppose Alice holds a shared key B_t and wants to share with Bob. For the preparation steps, let P, $Q \subseteq <r>$ be two subsets selected by Alice and Bob respectively and kept secretly. Note that all the elements in the subsets P and Q are commutes. Alice chooses $a \in B_1...B_{t-1}$ and two distinct elements $p_1, p_2 \in P$ secretly. Bob chooses $b \in D_{2n}$ and two distinct elements $q_1, q_2 \in Q$ secretly.

In order to share the exchange key B_t, we need to share the private keys a and b first since the keys a and b are needed to compute the exchange key B_t. The ten steps involved using the proposed computational complete decomposition of D_{2n} of order t search problem are shown in Figure 1.

RESULTS AND DISCUSSION

PERFORMANCE ANALYSIS

When two parties want to exchange the encrypted message, then there will be several steps of encrypting and decrypting the messages which are to be sent and received respectively. We use non-abelian dihedral groups to construct the proposed key exchange protocol. Since the elements in the dihedral groups are not commute, it will take longer steps to complete the computational process as compare to the key exchange protocol using abelian groups. Suppose Alice holds a shared key B_t and wants to share with Bob. Figure 1 shows that there are eight steps involved for sharing both secret keys a and b selected by Alice and Bob respectively. Since $a \in B_1...B_{t-1}$, $b \in D_{2n}$ and there are $2n$ distinct elements in D_{2n}, we note that the probability of guessing the correct a and b are close to 0 as n increases. Bob will be able to extract the exchange key B_t using the selected value of n from the dihedral groups published earlier together with the private keys. Any potential adversaries without the published information in the initial stage will be not be able to compute the exchange keyB_t.

SECURITY ANALYSIS

Since the communication network is insecure, we need to protect against potential adversaries. Suppose that there exists an adversary John that trying to attack our proposed protocols and he might be an active or passive adversary. If John is a passive adversary, then his actions are restricted to eavesdropping on messages that are transmitted over the network. John might use two attacks:

- Active Attack: John attempts to masquerade as other users in the network.

- Passive Attack: John attempts to determine partial information about the key exchanged by the users in the network.

We discuss the security of our proposed schemes based on these attacks. In the active attack, we assume that John is masquerade as Bob. John should have $b' \in D_{2n}$, and two distinct elements $q_1', q_2' \in \langle r \rangle$. Therefore, John shall receive a from Alice in Step 4 and Alice shall receive b' from John in Step 8. Alice and John calculate ab' and Alice computes $rB_t(ab)$. However, John is unable to compute B_t since he has no information about the value of n which can be obtained in the information published earlier to proceed on the last step. The probability of guessing the value of n is close to 0 as n increases. Thus, the proposed protocol is secure under active attack.

Next, we shall discuss the security of protocol under passive attack. There are total of six messages sent are related to a and b respectively, where the messages does not reveal any information about a and b. Without a and b, John is not able to compute B_t, and it is computationally infeasible.

CONCLUSION

Group covering of G is defined as manipulating the subsets of G such that it covers G. Complete decomposition of G of order t is one type of the group coverings and it has applications in cryptography. In this paper, we focus on a non-abelian group, which is the dihedral group D_{2n} for positive integer $n \geq 3$. We show that there exists a complete decomposition of D_{2n} of order t for $t \in \{2,3, \ldots, n\}$.

For the applications in cryptography, we propose a computational complete decomposition of non-abelian group of order t search problem. Given B_1, ..., B_{t-1} and G where the subsets product $B_1...B_{t-1}$ is a proper subset of G. We need to find B_t such that the subsets product B_1 ... $B_t = G$, where B_1, ..., $B_t \subseteq G$ and all the subsets are pairwise disjoint. Let G be the dihedral group D_{2n} of order 2_n. We propose a key exchange protocol based on the complete decompositions of dihedral groups of order t. The subsets B_1, ..., B_{t-1} and the dihedral groups D_{2n} is selected and published to both Alice and Bob. Suppose Alice holds a shared key B_t and wants to share with Bob. To ensure that the shared key B_t being communicated between the authorized parties, Alice will select a private key a and Bob will select a private key b secretly. The four main steps involved to share the shared key B_t include the preparation steps, sharing the private key a, sharing the private key b and finally exchange the shared key B_t. Bob will be able to extract the key B_t using the selected value of n and shared keys a and b.

We must prevent any potential adversaries to more secure communication network. The security of our proposed scheme is discussed under both active and passive attacks. Our scheme is secure since we didn't share any keys directly and the scheme is constructed using non-abelian group with more secure steps.

ACKNOWLEDGEMENT

The research has been carried out under Fundamental Research Grant Scheme project FRGS/1/2017/STG06/UTAR/02/3 provided by Ministry of Higher Education of Malaysia.

DECLARATION OF COMPETING INTEREST

None.

REFERENCES

Boyd, C. & Anish, M. 2003. *Protocols for authentication and key establishment*. Springer Berlin Heidelberg.

Baba, S., Kotyada, S. & Teja, R. 2011. A non-abelian factorization problem and an associated cryptosystem. *Cryptology EPrint Archive Report* 2011/048.

Chin, A.Y.M. & Chen, H.V. 2017. Covering finite groups by subset products. *Ars Combinatoria* 131: 3-9.

Chin, A.Y.M. & Chen, H.V 2018. Complete decompositions of finite abelian groups. *Applicable Algebra in Engineering, Communication and Computing* 30(3): 263-274.

Cong, Y., Hong, H., Shao, J., Han, S., Lin, J. & Zhao, S. 2019. A New Secure Encryption Scheme Based on Group Factorization Problem. *IEEE Access* 7: 168728-168735.

Diffie, W. & Hellman, M.E. 1976. New direction in cryptography. *IEEE Transaction on Information Theory,* 22(6): 644-654.

ElGamal, T. 1984. A public key cryptosystem and a signature scheme based on discrete logarithm. IEEE Transaction on Information Theory, 31(4): 469-472.

Gu, L. & Zheng, S. 2014. Conjugacy systems based on nonabelian factorization problems and their applications in cryptography. *Journal of Applied Mathematics*, 2014(6): 1-10.

Gupta, S., Kumar, A. & Kumar, N. 2018. Design of ECC based authenticated group key agreement protocol using self-certified public keys. *4th International Conference on Recent Advances in Information Technology* (RAIT), Dhanbad, 2018, 1-5.

Lee, E. 2005. A property for cryptography based on infinite groups. Trends in 157 *Mathematics*, 8(1): 155-166.

Magliveras, S.S., Stinson, D.R., van Trung, T. 2002. New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. *Journal of Cryptology* 15: 285-297.

Magliveras, S.S. 2002. Secret and public-key cryptosystems from group factorizations. *Journal of Cryptology* 25: 1-12.

Rawat, A.S., & Deshmukh, M. 2019. Efficient extended Diffie-Hellman key exchange protocol. International Conference on Computing, *Power and Communication Technologies* (GUCON) 2019, 447–451.

Rivest, R.L., Shamir, A. & Adleman, L. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120-126.

Shor, P.W. 1997. Polynomial-time algorithm for prime factorization and discrete logarithms on quantum computer. *SIAM Journal on computing*, 26(5): 1484-1509.

Szabo, S. & Sands, A.D. 2009. Factoring groups into subsets. CRC Press.

Wong, D.C.K, Wong, K.W. & Yap, W.S. 2018. Exhaustion 2-subsets in dihedral groups of order 2p. Asian-European *Journal of Mathematics, World Scientific Publishing Company* 11(3): 1-13.

Zhang, F., Safavi-Naini, R. & Susilo, W. 2004. *An efficient signature scheme from bilinear pairings and its application.* Public Key Cryptography – PKC 2004. Lecture Notes in Computer Science, vol 2947. Springer, Berlin, Heidelberg.

Zhou, Y. 2017. Multiple factorizations of cyclic groups. *Discrete Mathematics* 340 (7): 1581-1583.